

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
 INFORMATION ASSOCIATED WITH
 HONGJIN TAN's ONEDRIVE ACCOUNT
 ASSOCIATED WITH USER CID
 1BF4BD72B32D757D AND EMAIL
 ADDRESS lewistan90@hotmail.com, THAT IS
 STORED AT PREMISES CONTROLLED BY
 MICROSOFT

Case No. 19-mj-51-FHM

FILED
 MAR 01 2019
 Mark C. McCartt, Clerk
 U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1832(a)	Theft of Trade Secrets
18 U.S.C. § 1030(a)(1)	Fraud and Related Activities in Connection with Computers

The application is based on these facts:

See Attached Affidavit by Stephen Carnevale, SA/FBI

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature


Stephen Carnevale, SA, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 3-1-19

City and state: Tulsa, OK



Judge's signature

US Magistrate Judge Frank H. McCarthy

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
HONGJIN TAN's ONEDRIVE
ACCOUNT ASSOCIATED WITH USER
CID 1BF4BD72B32D757D AND EMAIL
ADDRESS lewistan90@hotmail.com,
THAT IS STORED AT PREMISES
CONTROLLED BY **MICROSOFT**

Case No. _____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Stephen Carnevale, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by **MICROSOFT**, an [electronic communications service/remote computing service] provider headquartered at Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **MICROSOFT** to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the Oklahoma City Field Office, Tulsa Resident Agency. As a Special Agent, my duties include investigating violations of federal criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in numerous investigations working alongside experienced law enforcement officers at both the federal and

local level. My investigations include, but are not limited to, counterterrorism, computer intrusions, drug and gang violations, violent crimes, and counterintelligence.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1832(a) – Theft of Trade Secrets and Title 18, United States Code, Section 1030(a)(1) – Fraud and Related Activities in Connection with Computers have been committed by **Hongjin Tan**. There is also probable cause to search the information described in Attachment A for [[evidence, instrumentalities, contraband, and/or fruits]] of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING MICROSOFT ONEDRIVE

6. **ONEDRIVE** is a Microsoft application that allows its users to store files on Microsoft’s servers. According to Microsoft’s website, at <https://products.office.com/en-us/onedrive-for-business/online-cloud-storage>, **ONEDRIVE** allows users to “Access, share, and collaborate on all your files from anywhere.”

7. In general, providers like **MICROSOFT** ask each of their subscribers to provide certain personal identifying information when registering for an ACCOUNT. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the ACCOUNT.

8. In some cases, ACCOUNT users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND CONCERNING COMPANY A

9. Company A was established in 1917, and is an international independent energy and petroleum corporation, focused on the exploration and development of petrochemical products and by-products, oil, and natural gas. Several years ago, Company A developed a cutting-edge Downstream Energy Market Product (hereafter referred to as Product A), and in the last year alone,

has earned an estimated \$1.4 to \$1.8 billion from the sale and distribution of the product in interstate and foreign markets. Currently, there are only two refineries in the world capable of manufacturing Product A, and one is located in the Northern District of Oklahoma.

10. Company A's technological research, development, and processes associated with the production of Product A are critical to its business and are considered sensitive proprietary information. This information (hereinafter referred to as the Trade Secret Information), would be of significant value to Company A's competitors, and is therefore protected through a multi-layered strategy involving both physical security, as well as password protected computer systems.

11. Company A restricts access to the facility where Product A is produced. Magnetic card readers are utilized to gain access to the main building, and are again required to enter individual research divisions within. Only employees with an operational need-to-know are granted access to Trade Secret Information. Additionally, as a condition of their employment, all personnel are required to sign a non-disclosure agreement specifically prohibiting the distribution of any confidential and proprietary information, and or research products to other companies, persons, or countries.

12. Company A also has multiple data security policies in place stipulating all information created, sent, received, or stored on Company A's electronic resources is company property, and all activity on Company A's electronic resources is subject to monitoring. These policies prohibit employees from transmitting, receiving, or storing company information outside Company A's electronic resources.

13. Company A has advised investigating agents that **MICROSOFT ONEDRIVE** is not an authorized file storage or file sharing system for work being conducted at Company A.

BACKGROUND CONCERNING HONGJIN TAN

14. On 04/21/2017, Company A hired Hongjin Tan, a citizen of The People's Republic of China, as a research engineer in their battery development division in the Northern District of Oklahoma. According to the resume Tan provided Company A, Tan received a Bachelor of Science Degree in Physics from Nanjing University in Nanjing, China (2006), and a Master's Degree and Doctorate Degree from the California Institute of Technology in Pasadena, California (2011). While employed with Company A, Tan was responsible for the development of battery technology through the utilization of Company A proprietary information.

PROBABLE CAUSE

15. On 12/13/2018, at approximately 12:19 p.m. Eastern Time, Company A notified the FBI regarding possible theft of trade secrets at their primary facility in the Northern District of Oklahoma. According to a Company A representative, on 12/12/2018 at approximately 10:30 a.m., Tan provided his two weeks' notice to his supervisor, and said he was returning to China to take care of his aging parents. Tan said he did not currently have a job offer, but was negotiating with several battery companies in China. Tan's sudden and unforeseen resignation, coupled with the possibility of Tan seeking employment with a competitor, prompted Company A to revoke his access to company systems, and conduct a Systems Access review of his computer activity.

16. During the review, Company A security specialists noted Tan had recently accessed hundreds of files considered to be outside the scope of his employment. Among these files were multiple documents pertaining to the technical processes involved in the production of Product A, its use in cell-phone and lithium-based battery systems, as well as Company A's marketing strategy for Product A in China.

17. Security personnel escorted Tan to his supervisor's office where he was advised he would not be allowed to finish his final two weeks of employment, and was no longer authorized to be on Company A's property. Tan's personal bag and keys were searched, and then he was escorted off the premises. At approximately 4:00 p.m. that afternoon, Tan sent the following text message to his supervisor:

... [Another Company A supervisor] was asking if there is anything I have with me associated with company IP. I have a memory disk that contains lab data that I plan to write report on, and papers/reports I plan to read at home. Now that I have been exited from (COMPANY A), can you check what is the best way of handling the information and how sensitive they are? Can I still read the papers/reports from the memory disk?

After receiving the above text from Tan, Tan's supervisor asked him to return the flash drive to Company A. At approximately 5:15 p.m. on 12/12/18, Tan returned to the Research Technology Center at Company A, where he provided a personally owned USB flash drive to his supervisor. Tan's supervisor confirmed at no point was he issued a flash drive, nor was he authorized to utilize one over his company issued laptop to access work related information, especially information deemed to be outside his duties and responsibilities.

18. Using commercially available software, Company A security specialists reviewed the USB flash drive and discovered it contained data files (both deleted and undeleted) owned solely by Company A. Several of the documents were in fact marked "CONFIDENTIAL" or "RESTRICTED," and after further analyzation, it was determined these files in compilation with one another, would provide a competing company the technical know-how to produce Product A. The unauthorized distribution of this information would have tremendous impact to Company A in terms of technological and economic loss.

19. These specific files were deleted from the flash drive on 12/12/2018, the day of Tan's resignation. This in direct violation of the Confidential Information, Non-Disclosure and

Intellectual Property Agreement signed by Tan on 06/19/2018. Without prior written consent, employees are not to:

“disclose, use, reproduce, or transmit (except for the performance of his duties for Company A), or permit the unauthorized disclosure, use, reproduction or transmission of any Confidential Information during the period of his employment with Company A or at any time thereafter...and upon leaving the employ of Company A, take any records, memoranda, drawings, pictures, models, papers, notebooks, reports, computer disks or other similar media having Confidential Information in or on such media.”

20. Tan was reminded of this obligation every time he logged into his work computer by a warning banner which stated:

This is a private computer system to be accessed and used for (Company A) business purposes. By accessing, using and continuing to use this system or device, you agree to the terms of use. All access must be specifically authorized and used only in accordance with all applicable (Company A) policies. Unauthorized access or use of this system is prohibited and may expose you to liability under criminal and civil laws. Absent a separate written agreement, all non-personal information and content you create, store or collect on behalf of (Company A) or in the scope of your employment, on this computer system is the sole property of (Company A). To the extent permitted under local law, (Company A) reserves the right to monitor, access, intercept, records, read, copy, capture and disclose all information received, sent through or stored in this system or device, without notice, for any purpose and at any time.

21. On 12/13/2018, one of Tan’s co-workers filed a report with Company A security personnel. The co-worker said on 12/12/2018 while out to dinner with Tan, Tan told him he was leaving Oklahoma on 12/27/2018 to return to China. Tan said he had interviewed for a job with a Chinese company (hereafter referred to as Company B) during his last trip to China in September 2018, and had been in constant contact with the company since he was in graduate school at The California Institute of Technology.

22. According to their company website, Company B is an energy engineering company located in Xiamen, China, and has “developed two [battery] production lines so far, one for Li-ion battery cathode materials (such as lithium cobalt oxide, ternary cathode material, lithium

manganese oxide, lithium iron phosphate, etc.) and the other for NiMH battery anode material (Hydrogen storage alloy).”

23. International travel records for Tan from United States (U.S.) Customs and Border Protection and U.S. Department of Homeland Security confirm Tan traveled from the Dallas/Ft. Worth, Texas International Airport to Peking, China on 9/15/2018. Tan returned to the Dallas/Ft. Worth, Texas International Airport via the Beijing, China Capital International Airport on 9/30/2018.

24. On 12/14/2018, the FBI conducted social media inquiries related to Hongjin Tan. A Twitter account for Tan was identified which was associated with the email address of lewistan90@hotmail.com.

25. On 12/20/2018, pursuant to a federal search warrant signed and authorized by the Honorable Judge Jodi F. Jane, United States District Court for the Northern District of Oklahoma, a search was conducted at Tan’s residence located at 3312 Price Road, Apartment 5, Bartlesville, Oklahoma 74006, by personnel of the Federal Bureau of Investigation. During the search a laptop was seized by agents. During the search, a Lenovo Laptop/Tablet computer was seized. The laptop was then was forensically examined by technically trained FBI computer analysts.

26. A review of the evidence extracted from the personal laptop of Hongjin Tan found that on 12/13/2018, at approximately 11:02 a.m. (C.S.T) Tan, using an internet address associated with ONEDRIVE, accessed a key document regarding the production of Product A.

27. On January 14, 2019, a preservation letter was sent to **MICROSOFT** for account records related to lewistan90@hotmail.com. **MICROSOFT** was then served with legal process to identify ONEDRIVE accounts associated with lewistan90@hotmail.com.

28. On 2/12/2019 MICROSOFT responded to the above legal process and identified the following **ONEDRIVE** account: User CID 1BF4BD72B32D757D with an Owner's MSA Email Address of lewistan90@hotmail.com.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require **MICROSOFT** to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant.

31. Based on the aforementioned facts and circumstances, Affiant believes there is probable cause to suggest information maintained by **MICROSOFT** on the ONEDRIVE account with User CID 1BF4BD72B32D757D, with an Owner's MSA Email Address of lewistan90@hotmail.com, is associated with Hongjin Tan and may contain evidence, fruits, and or instrumentalities of violations of statutes as previously noted. I therefore respectfully request this Court to issue a search warrant for the location listed in Attachment A and the items listed in Attachment B.

32. Due to the fact **MICROSOFT**, upon receipt of this warrant, will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time, day or night. Additionally, pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

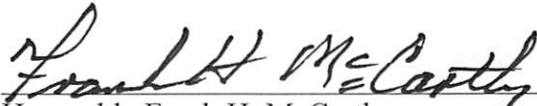
33. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Stephen Carnevale
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 3-1, 2019



Honorable Frank H. McCarthy
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

Hongjin Tan's **ONEDRIVE** Account associated with User CID 1BF4BD72B32D757D and Owner's MSA Email Address of lewistan90@hotmail.com that is stored at premises owned, maintained, controlled, or operated by **MICROSOFT**, a company headquartered at Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MICROSOFT

To the extent that the information described in Attachment A is within the possession, custody, or control of **MICROSOFT**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **MICROSOFT**, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **MICROSOFT** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the accounts;
- c. Account status, e-mail addresses provided during registration, and source of payment (including any credit or bank account number);
- d. The dates and times at which the accounts and profiles were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- e. All IP logs and other documents showing the IP address, date, time and duration of each login to the accounts;
- f. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- g. All location data associated with the accounts;

- h. All documents stored in or shared with other users through the account;
- i. All data and information deleted by the users;
- j. Accounts linked to the target accounts by cookies.
- k. All records pertaining to communications between **MICROSOFT** and any person regarding the account, including contacts with support services and records of actions taken.
- l. The identity of the person(s) who communicated with Hongjin Tan's **ONEDRIVE** Account associated with User CID 1BF4BD72B32D757D and Owner's MSA Email Address of lewistan90@hotmail.com about matters relating to theft of trade secrets, including records that help reveal their whereabouts.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1832(a) – Theft of Trade Secrets and Title 18, United States Code, Section 1030(a)(1) – Fraud and Related Activities in Connection with Computers involving **Hongjin Tan** since 1/1/2017 to present, including, for each account or identifier listed on Attachment A.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER'S] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by [PROVIDER], and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature